A SURVEY ON ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

Sonali U Nimbhorkar
Computer Science &Engineering
G.H.Raisoni College of Engineering
Nagpur, India
nimsonali12@yahoo.com

Dr.L.G.Malik
Computer Science &Engineering
G.H.Raisoni College of Engineering
Nagpur, India
lgmalik@rediffmail. com

Abstract— Now a days Elliptic Curve Cryptography is an promising type of public key cryptography that provides compensation by comparing with other public key algorithms like RSA, Diffie-Hellman key exchange and DSA. Understanding the use of public key cryptography which makes potential use of discrete logarithms problem. The security of ECC depends on the difficulty of Elliptic Curve Discrete Logarithm. The elliptic curve cryptography offers security more than sufficient with smaller key length. This paper provides brief explanation of Elliptic Curve Cryptography over Galois field.

Keywords-elliptic curve cryptography,security; finite field; elliptic curve;

I. INTRODUCTION

Cryptography is the art and science of hiding information in a systematic manner such that only authorized parties have access to right information. Cryptosystem broadly classified into two major categories, first is symmetric and other is asymmetric based on the concepts of key. In symmetric use same key is used for both encryption and decryption purpose. It is also called as secret key cryptosystems. While Asymmetric use two different keys, one is for encryption and another is used for decryption. Asymmetric is also known as public key cryptosystem. Elliptic curve cryptography was independently introduced by Neal Koblitz & Victor S.Miller in 1985 and 1987[12].Elliptic curve cryptography transforms a mathematical problem in to an applicable computer algorithm. Intractable problems are the center of public key cryptography and bring computationally demanding operations into a cryptosystem. curve cryptography (ECC) is based upon the algebraic structure of elliptic curves over finite field. The main advantage of ECC over other public key algorithms like RSA,DSA and Diffie-Hellman key exchange. It requires shorter key lengths for make sure the same level of security . For example , 160 bit key in ECC is considered to be as secured as 1024 bit key in RSA. Other than this ECC in particularly appropriate for wireless communication. Elliptic Curve Cryptography has become the cryptographic choice for networks and communication devices due to its size and efficiency benefits. Elliptic curve cipher uses very small keys and is computationally very efficient, which makes it ideal for the smaller, less powerful devices being used today by majority of individuals to access network services. Elliptic curve cryptography is more complex than RSA.As in RSA single encryption algorithms is used.ECC can be implemented in different ways.ECC uses arithmetic algorithms as the main objective operations for high level security functions such as encryption for gaining confidentiality and digital signature for authentication.ECC can be implemented in software and in hardware . ECC follows generic procedure like parties agree on publicly-known data items and each user generates their public and private keys[8][9][10][12][21][23] .

The rest of this paper is organized as follows : Section II describes overview of mathematical background for elliptic curve , definition of elliptic curves, major operations performed in elliptic curves cryptography in section III, discuss main security consideration for elliptic curve cryptography , comparison of ECC with RSA in section IV ,and section V analyze the implementation consideration of ECC for communication network, elliptic curve applications is explained in section VI. Finally ,conclusion is described in section VII.

II. MATHEMATICAL BACKGROUND

An elliptic curve over a field K of characteristic ≠ 2, 3 is given by an equation of the form

$$E : y^2 = x^3 + ax + b, \text{ with } a, b\ \varepsilon\ K\text{--------------------}1$$

$$\text{and}\quad \Delta = -16(4a^3 + 27b^2) \neq 0\text{------------------------}2$$

where Δ Discriminant function .
From equation 2 ,this equation represents a non-singular elliptic curve; otherwise ,the equation represented a singular elliptic curve .Discriminants of elliptic curves classified the curves into two types. In non-singular elliptic curve ,the equation $x^3+ax+b=0$ has three different roots ;in a singular elliptic curve the equation $x^3+ax+b=0$ does not have three different roots[8][9][10].
The set of K-rational points of an elliptic curve is
$E(K) = \{(x, y)\ \varepsilon\ K \times K ; y^2 = x^3 + ax + b\} U \{O\}$

In the general case, we consider the long Weierstrass form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a6,$$

where a1, a2, a3, a4, a6 ε K.

It is popularly known that *E* is an abelian group with the point ∞ serving as its identity element. The rules for group addition are summarized below[7][8].

The major operation in elliptic curve cryptography is the scalar multiplication .Scalar multiplication has the form k.P

$$k.\ P \rightarrow [k]P = P + \cdot\cdot\cdot + P,\ (k\ \text{times})$$

Where k is a positive integer ,

P is the point on elliptic curve .

Computation of k.P means adding point P exactly k-1 times to itself ,which resulting into other point Q on the elliptic curve .When points P and Q are given ,to recover k such operation is known as the elliptic curve discrete logarithm problem. In general scalar multiplication is performed by the combination of point additions and point doublings.

Elliptic curve arithmetic is defined in terms of underlying finite field which is a set of elements that have a finite order .The most popular finite fields used in ECC are Galois Fields (GF) that defined modulo prime number GF (p) or a binary extension fields GF (2^m)[8].

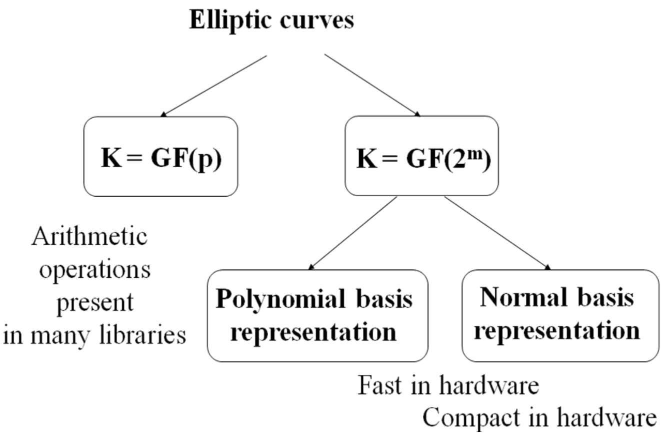
Elliptic curves
K = GF(p)
K = GF(2^m)
Arithmetic operations present in many libraries
Polynomial basis representation
Normal basis representation
Fast in hardware
Compact in hardware

Figure1. Classes of Elliptic Curves

As shown in figure 1 two families of elliptic curves are used in cryptographic applications like prime curves GF(p) and binary curves over GF(2^m).In prime curve ,use a cubic equation which takes variables and coefficients values in the set of integers from o to p-1 and performed the calculations using modulo p . In binary curve ,the variables and coefficients uses values in GF(2^m) and performed the calculations over GF(2^m).

Cryptography needs modular arithmetic for addition operation , algebraic structure like group and field. The group defines the set of the points on the elliptic curves and the addition operation on the points. The field defines the addition ,subtraction ,multiplication ,and division that are required for determining the addition of the points in the group.

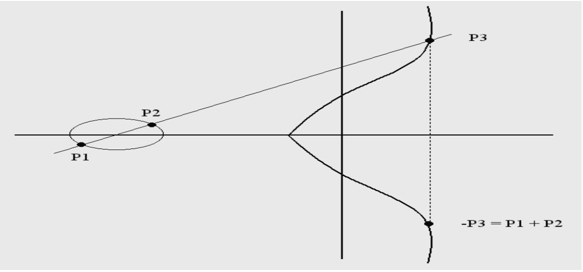

Figure2.Group laws on elliptic curve

Figure2 shows the addition of two points on an elliptic curve. Elliptic curves have the interesting property that adding two points on the elliptic curve results a third point on the curve. Therefore, adding two points, P1 and P2, gets us to point P3, also on the curve. Small changes in P1 or P2 can cause a large change in the position of P3.

Point addition is the addition of two points J and K on an elliptic curve to obtain another point L on the same elliptic curve as shown in figure 3and point doubling Point doubling is the addition of a point J on the elliptic curve to itself to obtain another point L as shown in figure 4.

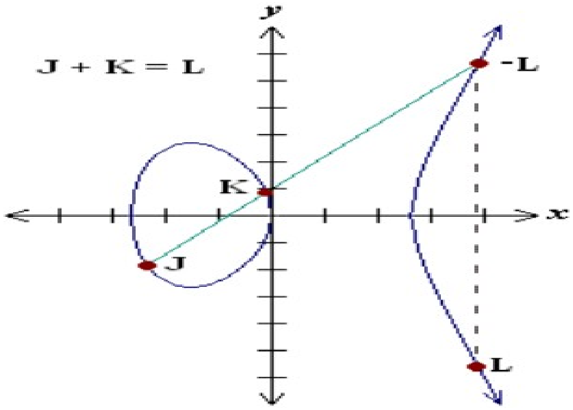

Figure3. Group laws of Elliptic Curve (point addition)

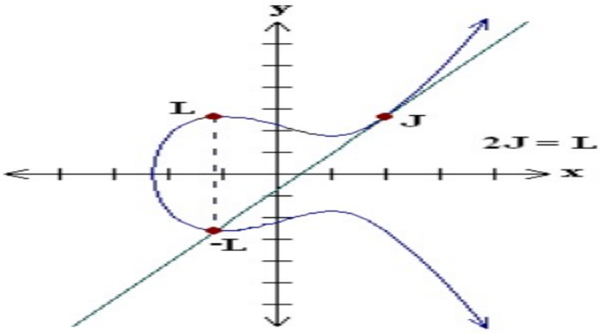

Figure4. Group laws of Elliptic Curve(point doubling)

III. ELLIPTIC CURVE CRYPTOGRAPHY

A. Scalar Multiplication

The most time consuming operation in elliptic curve cryptography is point multiplication or scalar multiplication , For speeding up this process, numerous approaches, methods, and algorithms exist, like Selection of an underlying finite field which is suitable for fast implementation in software as well as in hardware, Selection of a representation of the underlying finite field. The purpose is to select such representation, which provides the fastest arithmetic in the field. This is possible due to the existence of some representations of finite fields that have computational advantages over the other representations, Selection of an elliptic curve[2][6][21]. Numerous modifications of the general elliptic curve equation 1 , Selection of a point representation that the speed of point exponentiation. Point representations done using coordinates system can even be mixed to achieve best performance throughout the run of an exponentiation algorithm. Efficiency of an algorithm can be described from two basic points of view memory requirements and computational difficulty. Memory requirements are basically the needs of certain size of the memory for performing operation.

B. Schemes for Scalar Multiplication

There are different ways to implement scalar multiplication like Binary ,Signed digit representation(NAF),Montgomery method .There are three different phases to performed scalar multiplication .At the top level, select the method for computation the scalar multiplication ,middle layer decides underlying use of finite field and coordinate system and at the lower level finite field arithmetic is performed. Different possible ways to perform scalar multiplication are as follows[1][2][3][16][18] :

- Right to left binary method
- Left to right binary method
- Non Adjacent Form
- Width w Non Adjacent Form
- Joint Sparse Form
- Double and add form
- Addition chains
- Fibonacci and add
- Montgomery method

The binary method is simplest method used for scalar multiplication .It scans every bit of scalar k and depending upon bits value,0 or 1,it performs point doubling operation or both point doubling and point addition and an point addition. The Binary method consists of a point doubling operation if the key bit is ‘0’, and a point doubling followed by a point addition operation if the key bit is ‘1’. If the power pattern of point doubling is different from that of point addition, attackers can easily retrieve the secret key from a single power trace [3]. Montgomery and Double-and-Add-Always methods remove the conditional branches through executing a point doubling and an addition whatever the key bit is. Thus the Montgomery and Double-and-Add-Always methods are often used to defeat SPA attacks. Other SPA-resistant methods include the Double-and-Add-Balanced method, which balance point doubling and addition by means of dummy operations insertion in the Binary method[2][8].

The primary scalar multiplication method used by Ecclib was developed by Lopez and Dahab. This method has been measured by most researchers to be the most efficient Algorithm for polynomial bases because once the point is improved to Montgomery projective coordinates, Calculations can subsequently be performed only on x and z.Once the result has been computed, the resulting y value can be computed through post processing. Furthermore, it is very efficient as it requires only six multiplications per bit of the scalar and can be supplementary optimized to require only five multiplications per bit for Koblitz curves[6][20][21].

C. Various forms of coordinate system for point representation

A coordinate system is a organization which uses one or more numbers, or coordinates, to distinctively determine the position of a point or other geometric constituent on a manifold such as Euclidean space. The use of a coordinate system allows problems in geometry to be translated into problems about numbers and vice versa.

An elliptic curve can be represented by several coordinate systems [11]. Following are descriptions of coordinates system. Point additions(PA) and point doublings(PD) can be implemented using following coordinate system[5][6]

- Affine coordinate system
- Standard projective
- Standard projective and affine
- Jacobian projective
- Jacobian projective and affine
- Lopez –Dahab

The affine coordinates system considered the normal form Hessian curve without any projection to produce the value of the point doubling represented as P3= (x3, y3). By Using the point-slope (m) equation y=mx + c [6].

Where m is the gradient of line.

c is the y-intercept.

Affine coordinate system needs field inversion in the both Point additions (PA) and point doublings (PD),whereas other coordinate system do not need it. Inversions are very exclusive that can be take out by changing the representation of the points. In some different coordinate systems, points on a curve can be added without inversions[14][22].

$(x; y) \rightarrow (X; Y ; Z)$

Transformation: $x = X/Z^c$ and $y = Y /Z^d$

Where c ,d are multiplier parameters

D. Types of curves

There are two kinds of curves are given in general[10][12] :

- Pseudo-random curves are those whose coefficients are generated from the output of a seeded cryptographic hash.
- Special curves whose coefficients and essential field have been preferred to optimize the efficiency of the elliptic curve operations.

IV. SECURITY OF ELLIPTIC CURVE CRYPTOGRAPHY

As RSA depends on the difficulty of large-number factorization for its security, ECC depends on the difficulty of the large number discrete logarithm calculation. This is referred to as the Elliptic Curve Discrete Logarithm Problem (ECDLP). Elliptic curves for which the total number of points on the curve equals the number of essentials in the primary finite field are also considered cryptographically pathetic. Again the security of ECC depends upon how to calculate k when point is given in scalar multiplication [10][4].

TABLE I. EQUIVALENT KEY SIZES FOR SYMMETRIC ,ECC AND RSA

Symmetric scheme(key size in bits)	Elliptic curve cryptography based schemes (key size in bits)	RSA/DSA(modulus size in bits)
56	112	512
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

Table I shows the Comparison between symmetric and asymmetric algorithms such AES ,ECC ,and RSA . Same level of security ,data sizes ,encrypted message sizes and computational power .The security levels which is given by RSA can be provided by smaller keys of elliptic curve cryptosystem[3][21][17].

For providing security mechanism will require fundamental basic security services such as authentication, confidentiality, non-repudiation and message integrity. Authentication confirms the identity of the party involved in communication, confidentiality assures that only intended receiver should able to understand the contents of transmitted message ,message integrity guarantees that the messages is not altered and non-repudiation ensures proofers of communication[5][7][11] .

V. IMPLEMENTATION ISSUES IN ELLIPTIC CURVE CRYPTOGRAPHY

There are many issues to be discussed between the mathematical basis for an ECC scheme and a practical working ECC system like EC Parameters generation , Selection of Parameter set, Level of security, Interoperability, Performance, Application Level Issues, Device Level Issues .For ECC implementation following point of consideration should assemble[1][2][4][25]

- Exactness of methods available for optimizing finite field arithmetic like addition, multiplication, squaring, and inversion.
- Exactness of methods available for optimizing elliptic curve arithmetic like point addition, point doubling, and scalar multiplication.
- Application platform like software, hardware, or firmware.
- Constraints of a particular computing environment e.g., processor speed, storage, code size, gate count, power consumption.
- Constraints of a particular communications environment e.g., bandwidth, response time.

Efficiency of ECC is depends upon factors such as computational outlay ,key size ,band width ,ECC provides higher-strength per- bit which include higher speeds, smaller power consumption, bandwidth reserves, storage efficiencies, and smaller certificates[13][20].

VI. APPLICATIONS OF ELLIPTIC CURVE CRYPTOGRAPHY

Applications of ECC includes the implementation of ECC for web's security infrastructure ,integration in openSSL, and for the implementation cryptographic algorithms and protocols[1].

Many devices are constrained devices that have small and restricted storage and computational power ,for constrained devices ECC can be applied[3][11].ECC can be functional For wireless communication devices like PDA's ,multimedia cellular phones .It can be used for security of Smart cards ,wireless sensor networks ,wireless mesh networks. Web servers that need to handle many encryption sessions. Any kind application where security is needed for our current cryptosystems. In public-key cryptosystem for secret key sharing offers Diffie-Hellman protocol ,in order to implement Diffie-Hellman protocol scalar multiplication is used[1][2][18].

VII. CONCLUSION

Elliptic curve systems are progressively more seen as an alternative to RSA, relatively than a replacement. The primary motive for the magnetism over RSA and DSA is that the best algorithm known for solving underlying use of ECDLP which takes fully exponential time than other public key cryptosystem. There are prospective advantages, particularly when used in devices with limited processing capability and/or memory. Representative applications includes m-commerce (e.g. mobile phone, hand-held devices) smart card systems, e-commerce and banking applications (e.g. SET) internet based applications (e.g. SSL) .There are, however, some problems and issues that are inhibiting the widespread adoption of elliptic curve systems[18][19][3] [13].

References

[1] Andrej Dujella "Applications of Elliptic Curves in Public Key Cryptography "Basque Center for Applied Mathematics and Universidad del Pais Vasco / Euskal HerrikoUnibertsitatea, Bilbao, May 2011.

[2] Moncef Amara ,Amar siad "Elliptic Curve Cryptography and its application"7th international workshop on systems ,signal processing and their applications(WOSSPA)IEEE 2011

[3] Tingding Chen, Huiyun Li, Keke Wu, Fengqi Yu "Evaluation Criterion Of Side-Channel Countermeasures For Elliptic Curve" 978-0-7695-3906-5/09 2009 IEEE.

[4] Philip Hines"Improvements to an Efficient Implementation of an Elliptic Curve Cryptosystem over a Binary Galois Field in the Polynomial Basis" Hines_Summer_2007_report.pdf

[5] Zhi Li, John Higgins, Mark Clement " Performance of Finite Field Arithmetic in an Elliptic Curve Cryptosystem"

[6] Fahad Bin Muhaya, Qasem Abu Al-Haija, and Lo'ai Tawalbeh" Applying Hessian Curves in Parallel to improve Elliptic Curve Scalar Multiplication Hardware".International Journal of Security and Its Applications Vol. 4, No. 2, April, 2010

[7] Samta Gajbhiye, Monisha Sharma, Samir Dashputre "A Survey Report on Elliptic Curve Cryptography" International Journal of Electrical and Computer Engineering (IJECE) Vol.1, No.2, December 2011, pp. 195~201 ISSN: 2088-8708.

[8] D. Sravana Kumar "CRYPTOGRAPHIC PROTOCOLS USING ELLIPTIC CURVE OVER FINITE FIELDS "International Journal of Engineering Science and Technology (IJEST) ISSN : 0975-5462 Vol. 4 No.01 January 2012

[9] Behrouz A Forouzan,Debdeep Mukhopadhayay "A text book of Cryptography and Network security",second edition 2011.

[10] William Stallings, "A text book of Cryptography and Network security", Principles and practices, Pearson education, fourth edition 2007.

[11] Xue Sun ,Mingping Xia "An improved proxy signature based on elliptic curve cryptography" DOI10.1109/ICCCS.2009.36

[12] www.certicom.com

[13] Jithra Adikari "Efficient Algorithms For Elliptic Curve Cryptography" Ph.D Thesis , Department Of Electrical & Computer Engineering,Calgary University, Alberta January, 2011.

[14] E.Munivel,Dr G M Ajit "Efficient Public Key Infrastructure Implementation in Wireless Sensor Networks" 2010 IEEE.

[15] A. Chandrasekar, V.R. Rajasekar & V. Vasudevan "Improved Authentication and Key Agreement Protocol Using Elliptic Curve Cryptography" International Journal of Computer Science and Security (IJCSS), Volume (3): Issue (4)

[16] Vassil Dimitrov, Laurent Imbert, And Pradeep K. Mishra "The Double-Base Number System And Its Application To Elliptic Curve Cryptography"MATHEMATICS OF COMPUTATIONS 0025-5718(07)02048-0,Article electronically published on December 11, 2007

[17] Mathias Schmalisch, Dirk Timmermann "Comparison of Algorithms for Finite Fields of *GF*(2*m*)",The IASTED International Conference on Communication, Network, and Information Security.CNIS 2003, December 10-12, 2003New york,USA**.**

[18] Dr.R.Shanmugalakshmi ,M.Prabu" Research Issues on Elliptic Curve Cryptography and Its applications"IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.6, June 2009.

[19] Michael Naehrig "Pairings on elliptic curves – parameter selection and efficient computation", Workshop on Elliptic Curve Computation ,Redmond, 19 October 2010

[20] Pardeep Malik "Elliptic Curve Cryptography For Security Inwireless Networks"Statistics 2011 Canada: 5th Canadian Conference in Applied Statistics/ 20th conference of the Forum for Interdisciplinary Mathematics -Interdisciplinary Mathematical Statistical Techniques, July 1-4-2011, Concordia University, Montreal, Quebec, Canada.

[21] Guicheng Shen ,Bingwu Liu"Research on Efficiency of computing kP in Elliptic Curve System" .,supported by funding project for science and technology program Beijing,2010 under grant numberKM20101010037002.

[22] SECG SEC1, "Elliptic Curve Cryptography, Standards for Efficient Cryptography Group, ver. 2, 2009, http://www.secg.org/download/aid-780/sec1-v2.pdf.

[23] Sheueling Chang, Hans Eberle, Vipul Gupta, Nils Gura, Sun Microsystems Laboratories "HowECCWorks-USLetter.pdf

[24] http://cse.iitkgp.ac.in/~debdeep/pres/TI/ecc.ppt

[25] Abdahossein rezai,parviz kashvarzi "high performance implementation approach of elliptic curve cryptosystem for wireless network applications,978-1-61284-459-6/11,IEEE 2011